ST BARNABAS CHURCH SUTTON

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

Statement of Intent

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. How the church obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, has the right to know how the information about them is used. The General Data Protection Regulation requires the church to strike the right balance in processing personal information so that an individual's privacy is protected while providing the services they expect. Applying the principles to all information held by the church should achieve this balance and help comply with the legislation.

We have record keeping systems in place that meet legal requirements; our means of storing and sharing that information take place within the framework of the General Data Protection Regulation.

General Data Protection Regulation principles

To comply with the regulation, the church must observe the eight 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up-to-date
- Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that the church must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data.

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information.

The General Data Protection Regulation principles apply to all information held electronically or in paper files.

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential.

Sensitive personal data relates to:

- race and ethnicity
- political opinions
- religious beliefs
- membership of trade unions
- physical and mental health
- sexuality
- criminal offences

What must the church do?

- We are registered with the ICO (Information Commissioner's Office)
- We have a nominated individual as the 'Data Protection Officer'

Data Breaches

In the event of a personal data breach, the Data Protection Officer should be notified immediately and an investigation carried out. If the data breach is considered to be serious (eg, theft of data poses a high risk to the individuals involved) then informing the ICO within 72 hours is compulsory.

Individual Rights

The General Data Protection Regulation includes the following rights for individuals :

- the right to be informed
- the right of access
- the right to rectification
- The right to erasure
- the right to strict processing
- the right to data portability
- the right to object, and
- the right not to be subject to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information the church holds on them - this is known as a Subject Access Request (SAR) and includes all and any information held by the church.

- SARS must be responded to within 1 month of receipt
- The SAR should be made in writing by the individual making the request
- The church can refuse or charge for requests that are manifestly unfounded or excessive

Office Holder's Responsibilities

Need to know and understand:

- How to manage, keep and dispose of data
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

Information and IT Equipment Acceptable Usage

Acceptable Usage covers the security and use of all church information and IT equipment. In addition the use of personal IT devices for church business.

Computer Access Control - Individual's Responsibility

Access to IT equipment must be password protected by at least 'one-factor' and preferably 'two-factor' eg, an unlock code plus an additional password.

Individuals must not:

- Leave their user accounts logged in at an unattended and unlocked computer
- Leave their password unprotected (eg, writing it down)

Internet and email Conditions of Use

Emails should be sent 'bcc' to undisclosed recipients unless the addressees already have access to each other's addresses, or specific permission has been given.

Individuals must not:

- Place any information in the Internet that relates to the church, alter any information about it, or express any opinion, or purport to speak for the church, unless they are specifically authorised to do so
- Send unprotected sensitive or confidential information externally.

Clear Screen Policy

- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended
- Care must be taken to not leave confidential material in printers or photocopiers
- All documents showing personal information matter must be disposed of using confidential waste bins or shredders
- Once electronic information is no longer required the files should be deleted securely and completely, such as by (1) deleting the files empty to the waste bin, (2) emptying the waste bin, then (3) defragragment the disc to overwrite the data.

Working Off-Site

- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used for personal data only with password protection.

It is your responsibility to report suspected breaches of security policy without delay to the Churchwardens and Data Protection Officer.

Access to staff personal data

- Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within one month.
- Should an employee request access to their personal data, the request must be addressed in writing to the Churchwarden. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within one month of the date of request.
- In the event of disagreement between an employee and a Churchwarden regarding personal data, the matter should be referred to the Chair of the PCC.
- The right of employees to see information held on them is extended to information held in paper record-keeping systems as well as computerised systems.
- There are some exemptions, for example, employees will not be able to see employment references about them supplied in confidence.

Adopted at PCC meeting ..... 2 October 2019 .....

Date .....

Review Date 2024

Revd QR Bibb

Chair